Rancang Bangun Realtime Web Application Firewall berbasis Deep Learning untuk Peningkatan Keamanan Aplikasi Web-Studi Kasus Badan Meteorologi, Klimatologi dan Geofisika = Development of Realtime Web Application Firewall based on Deep Learning to Improve Web Application Security-Case Study of the Meteorology, Climatology and Geophysics Agency

Rofif Zainul Muttaqin, author

Abstrak

Perkembangan teknologi yang terus berkembang mendorong penggunaan aplikasi web di berbagai layanan, namun terdapat berbagai kerentanan pada aplikasi web yang setiap saat dapat dimanfaatkan penyerang untuk melakukan serangan. Untuk menanggulangi hal ini, salah satu upaya yang dapat dilakukan ialah menerapkan Web Application Firewall (WAF) yang dapat melindungi aplikasi web. WAF umumnya bekerja berdasarkan aturan yang ditetapkan sebelumnya. Namun kelemahan sistem ini ialah serangan yang terus berkembang, serta dalam mengkonfigurasi aturan pada WAF, diperlukan pengetahuan mendalam terkait aplikasi yang ada. Teknologi kecerdasan buatan, baik machine learning (ML) atau deep learning (DL) memperlihatkan potensi yang baik dalam mengenali jenis serangan. Di dalam penelitian ini dibangun sebuah Real-time DL-based WAF untuk meningkatkan keamanan pada aplikasi web. Berbagai model ML dan DL diujicoba untuk melakukan tugas deteksi serangan web, mulai dari Support Vector Machine (SVM), Random Forest (RF), Convolutional Neural Network (CNN), dan Long Short-Term Memory (LSTM). Berdasarkan hasil pengujian, model CNN-LSTM meraih performa tertinggi yakni akurasi sebesar 98.61 %, presisi sebesar 99%, recall sebesar 98.08% dan f1-score sebesar 98.54%.. Dari hasil pengujian dengan web vulnerability scanner, performa DL-based WAF tidak kalah dengan ModSecurity WAF yang dijadikan sebagai pembanding. Dari hasil analisis, dapat disimpulkan bahwa penerapan DL-based WAF mampu meningkatkan keamanan pada aplikasi web.

.....The continuous development of technology drives the use of web applications in various services, but there are various vulnerabilities in web applications that can be exploited by attackers at any time. To overcome this, one effort that can be done is to implement a Web Application Firewall (WAF) that can protect web applications. WAF generally works based on pre-established rules. However, the weakness of this system is the evolving nature of attacks, and configuring rules on WAF requires in-depth knowledge related to existing applications. Artificial intelligence technology, both machine learning (ML) and deep learning (DL), shows good potential in recognizing types of attacks. In this research, a Real-time DL-based WAF was built to enhance security in web applications. Various ML and DL models were tested to perform the task of web attack detection, including Support Vector Machine (SVM), Random Forest (RF), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM). Based on the test results, the CNN-LSTM model achieved the highest performance, namely an accuracy of 98.61%, precision of 99%, recall of 98.08%, and f1-score of 98.54%. From the testing results with a web vulnerability scanner, the performance of the DL-based WAF is not inferior to ModSecurity WAF, which is used as a comparison. From the analysis results, it can be concluded that the implementation of DL-based WAF can improve the security of web applications.